Information Assurance and DoD:
A Partnership with Industry

Presented By:

Robert Lentz

Director, Information Assurance

OASD(C3I)

for the

ITAA InfoSec Committee Meeting

March 26, 2002

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 26-03-2002	2. REPORT TYPE Briefing	3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE	
Information Assurance and DoD: A Partnership with Industry Unclassified	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	
Lentz, Rpbert ;	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS OASD(C3I) xxxxx, xxxxxxx	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS OASD(C3I) ,	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See report.

15. SUBJECT TERMS
IATAC Collection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 22	19. NAME OF RESPONSIBLE PERSON email from Booz, Allen & Hamilton (IATAC), (blank) lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39.18

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 3/26/2002	3. REPORT TYPE AND DATES COVERED Briefing 3/26/2002

4. TITLE AND SUBTITLE
Information Assurance and DoD: A Partnership with Industry

5. FUNDING NUMBERS

6. AUTHOR(S)
Lentz, Robert

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

OASD(C3I)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

OASD(C3I)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

This briefing presents the information assurance environment, DoD's vision, the DoD IA community response and challenges, the DoD Industry Relationship, key influences on the DoD and a summary.

14. SUBJECT TERMS
IATAC Collection, information assurance

15. NUMBER OF PAGES

21

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED

Briefing Overview

• The environment-->push & pull; the evolution of threats & technology

• DoD's vision-->Decision Dominance enabled by network centric operations 'netcentricity'

• The DoD IA Community response & challenges

• The DoD - Industry Relationship

• Key Influences on the DoD - Industry Relationship
  • Policies
• Summary

The Changing Face of Cyber Threat

Current Situation Assessment

- Global access to information
- Networks emerging as centers of gravity
- Geographic and infrastructure boundaries meaningless
- Critical infrastructures/ sectors are targets
- Cyber response problematic
- Anonymity makes tracing difficult
- Technology has given rise to new threats
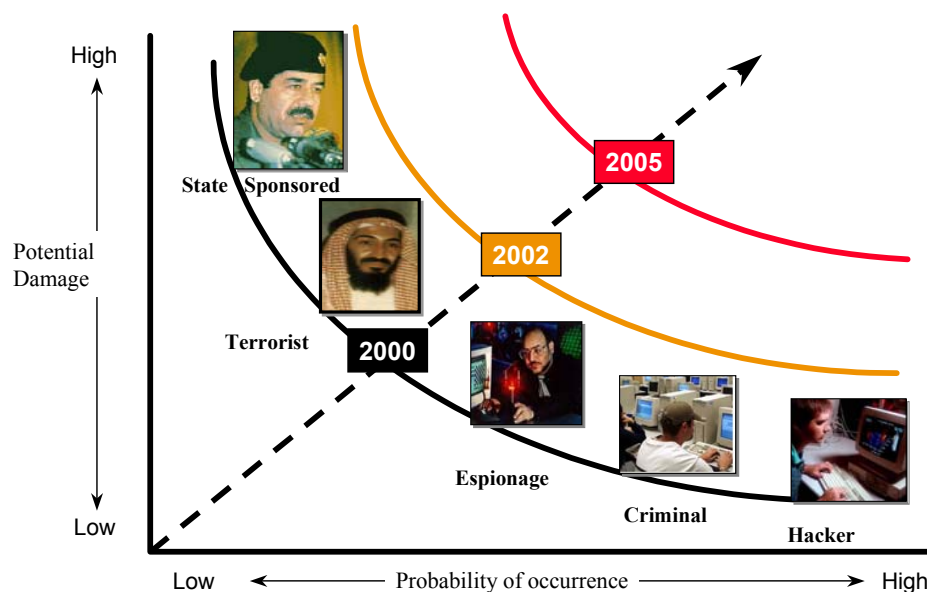
Source: 1996 DSB Summer Study

Individual Hacker	Criminal / Disgruntled Employee	Terrorist / Nation-State
Intrusion	*Crime*	*Attack*
• Access • Challenge • Ego	• Theft • Alteration • Destruction	• Exploitation • Degradation • Destruction

Most Likely   **Least Likely**

Annoyance   **Strategic Impact**

Gartner's Top 10 Technologies
2002-2007

- Gartners top 10 technologies (2002-2007)
  - Biometric authentication
  - Speech recognition
  - web services
  - portals
  - always-on wireless data & communications
  - converged networks
  - digital wallets & interest portfolios
  - wireless LAN
  - privacy management technology
  - instant messaging
- Venture Capital "hot" investment areas for 2002: INFRASTRUCTURE
  - network, systems, security and data infrastructure

What are the security implications of these technologies?!

Enabling Full Spectrum Dominance

DoD Vision

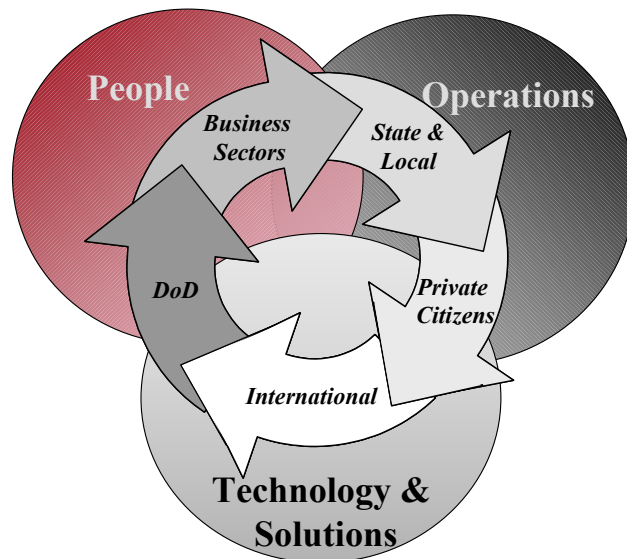Dedicated individuals and innovative organizations transforming the joint force for the 21st Century to achieve *Full Spectrum Dominance*:

- Persuasive in peace
- Decisive in war
- Preeminent in any form of conflict

Information Assurance
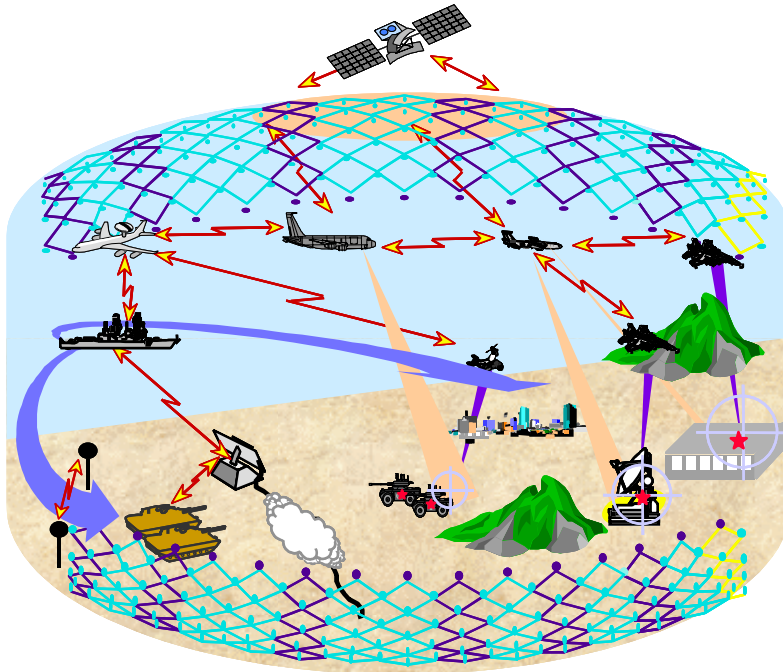
One Team – One Vision

Future DoD Operations
"NetCentricity"

- *Defines* future warfare transformed by information technology
- *Focuses* on battlefield entities, information flows, and their interactions
- *Describes* strategy, operations, tactics & doctrine that takes advantage of information technology

Requires a Global Information Grid
- Massed effects not forces
- Delivers "Power to the Edge"
- Highly aware forces
- Increased operational speed & agility
- Optimized environment for improved decision making (C2)

Seeks to reduce or eliminate the constraints of space & time

"Netcentricity"
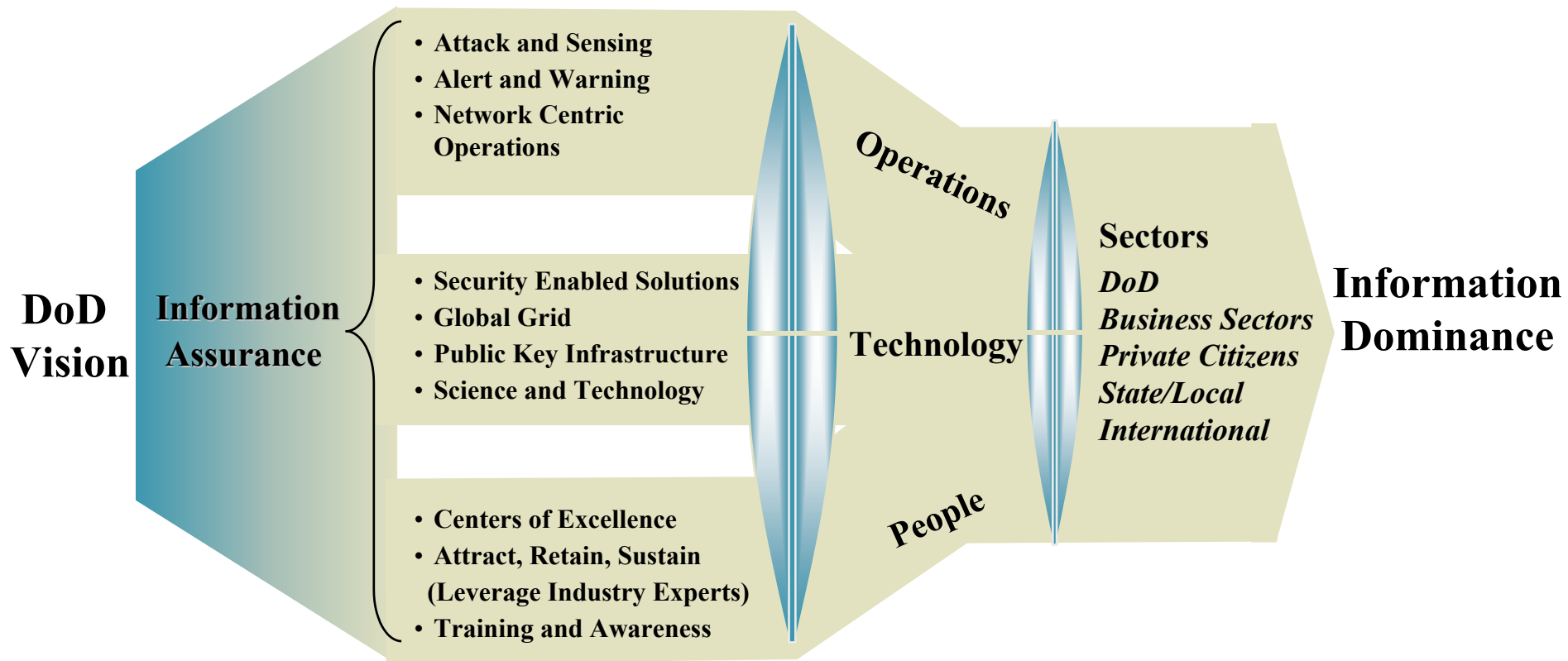## *Increases Demand for New & Improved IA Capabilities*

- **Embedded IA services/management** in nodes/links
  - Adaptive, automated configuration and remote operation of components/systems
- **High confidence**, scaleable supporting infrastructures
- **New skill sets of flexibility**, coping with higher levels of ambiguity and uncertainty and to operate under growing levels of pressure
- **Well integrated assurance tools** into development, deployment, employment, support mechanisms
  - ID need/opportunity
  - Define response
  - Design implementations
  - Develop capabilities
  - Deploy (deliver) result
  - Employ (use)
  - Support (maintain, sustain)
  - Enforce, assess-evaluate, insight-oversight

DoD Information Assurance Model

Information Assurance enables Information Dominance

DoD Vision

Information Assurance

- Attack and Sensing
- Alert and Warning
- Network Centric Operations

- Security Enabled Solutions
- Global Grid
- Public Key Infrastructure
- Science and Technology

- Centers of Excellence
- Attract, Retain, Sustain (Leverage Industry Experts)
- Training and Awareness

Operations

Technology

People

Sectors
DoD
Business Sectors
Private Citizens
State/Local
International

Information Dominance

Vision & Goals

VISION: "Mission Dominance through Dynamic IA"

KEY TENETS:

- Globalization mandates **partnerships** (Allies & Industry)
- Consumer IT markets heavily influence operational requirements **(develop proactive IA solutions)**
- IA is an enterprise-wide capability that demands decisions from an enterprise perspective (**process change**)
- Users demand agility, transparency, & intrinsic trust in the global information grid. **(user driven)**

GOALS:

- PROTECT INFORMATION: Maintaining the essential qualities of information.
- DEFEND NETWORKS: Assure vulnerabilities are not exploited; we are aware of exploitation attempts AND take action to avert risks.
- CREATE IA SITUATIONAL AWARENESS/C2: Build Confidence in our ways & means; respond faster than our adversaries.
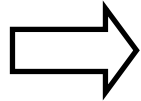- MAINTAIN ROBUST INFRASTRUCTURES: Enable the ability to adapt to uncertainties and ambiguities in the environment.

IA Strategic Focus (By Domain)
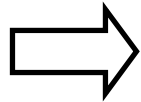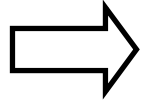
Major Focus

• **GLOBAL Domain** → **Assured collaboration with Allies and in Coalition operations**
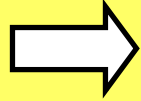
• **US Domain** → **Appropriate ventures with the private sector - maintaining cutting edge solutions vis a vis privacy issues**

• **FEDERAL Domain** → **Influence information assurance in homeland defense**

• **DEFENSE Domain** → **Protect Information, Defend Networks, Create IA Situational Awareness/C2, Maintain Robust Infrastructures**

Develop policies _concurrently_ with the implementation of a capability

A New IA Strategic Framework

Consumer Focused, Collaborative Base, Dynamic in Nature

INVESTMENT STRATEGIES

Sustain   **Transform**   **Leap-Ahead**

ENDURING GOALS

Protect Information

Defend Networks

Create **IA Situational Awareness/C2**

Maintain **Robust Infrastructures**

SETS OF CAPABILITIES
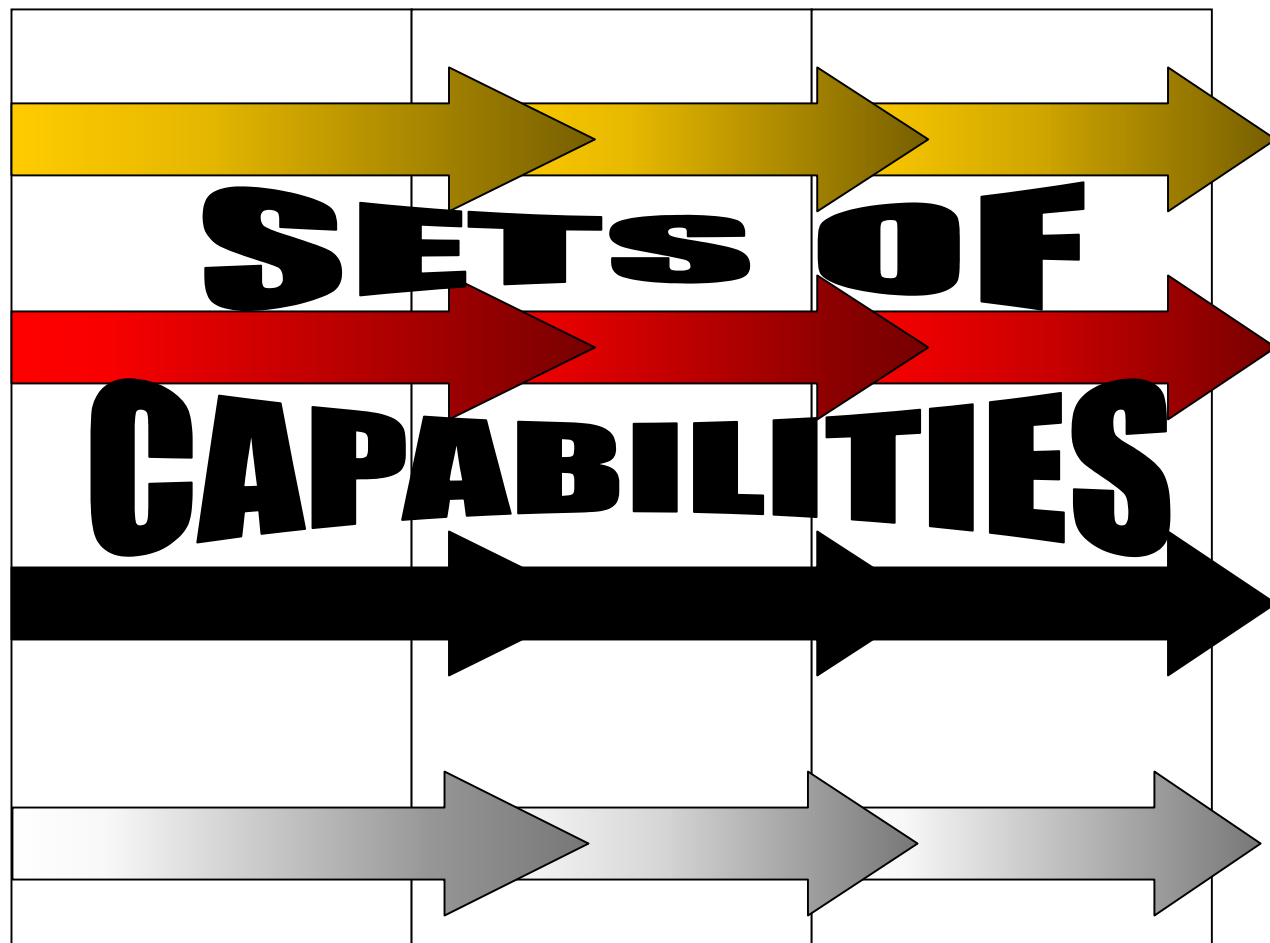
Information Dominance - *Operations*
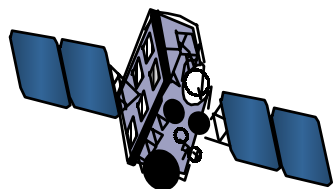
Alert and Warning

The Challenge:
To share critical vulnerability information rapidly with international and domestic partners.

Attack and Sensing

The Challenge:
Early detection of malicious activities.

Network Centric Operations

The Challenge:
To establish a common operational picture and avoid information stovepipes.

Information Dominance - *People*

Centers of Academic Excellence in IA Education

The Challenge:
To develop the future workforce and increase the number of professionals with IA expertise.

GOAL: ATTRACT, SUSTAIN, AND RETAIN IA PROFESSIONALS
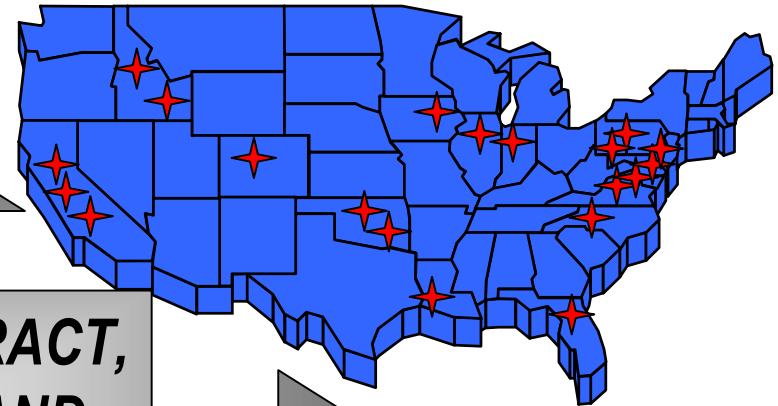
Training and Awareness

The Challenge:
To keep the current workforce ahead of the IT curve with new educational programs and professional IA training.

Information Dominance - *Technology*

Science and Technology
The Challenge:
To rapidly develop and implement innovative security solutions

Global Grid
The Challenge:
To keep pace with information demands while ensuring security.
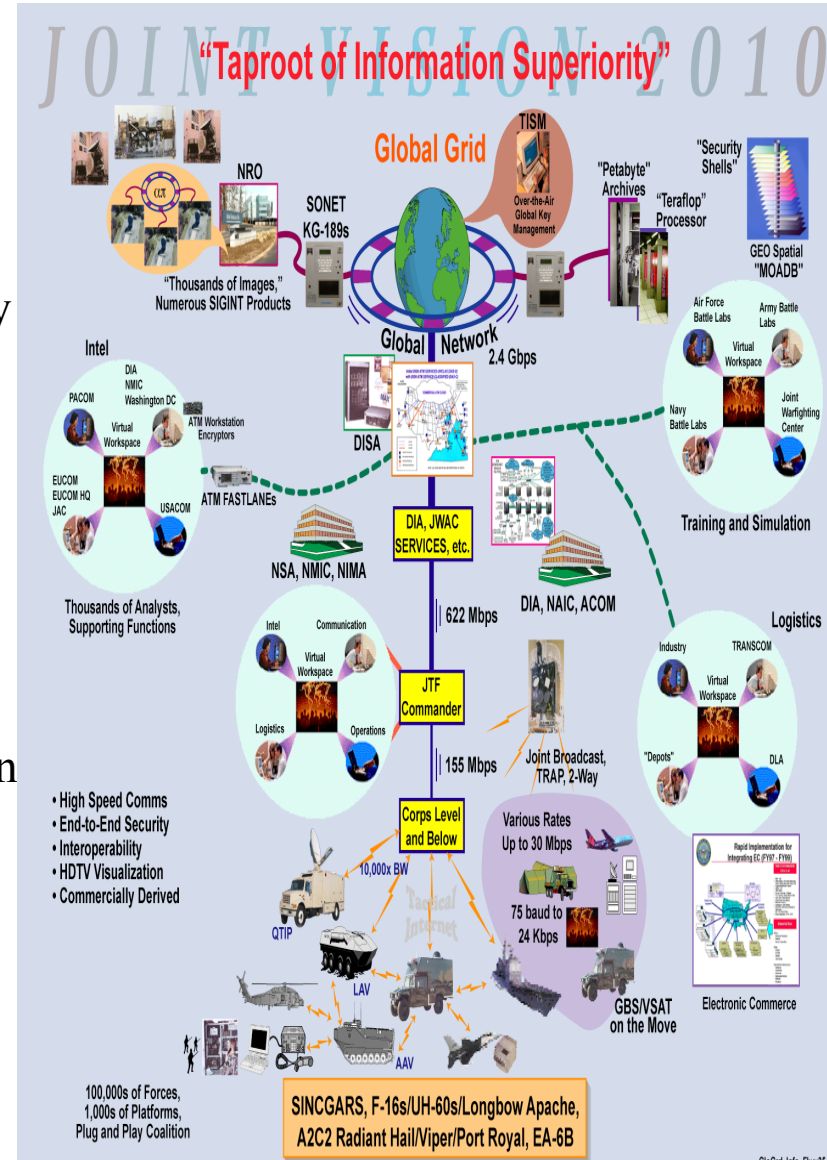
Information Dominance - *Technology*

Security Enabled Solutions

The Challenge:
To acquire products and applications that contain security robustness.

Remote Dial-In User

Telephone

Defend Networks and Infrastructure

Defend Computing Environment

Local Enclave

Switched Tele Network

Wireless

Defend Enclave Boundary

Desktop

Data Network

Combat Radio

Server

Public Key Infrastructure
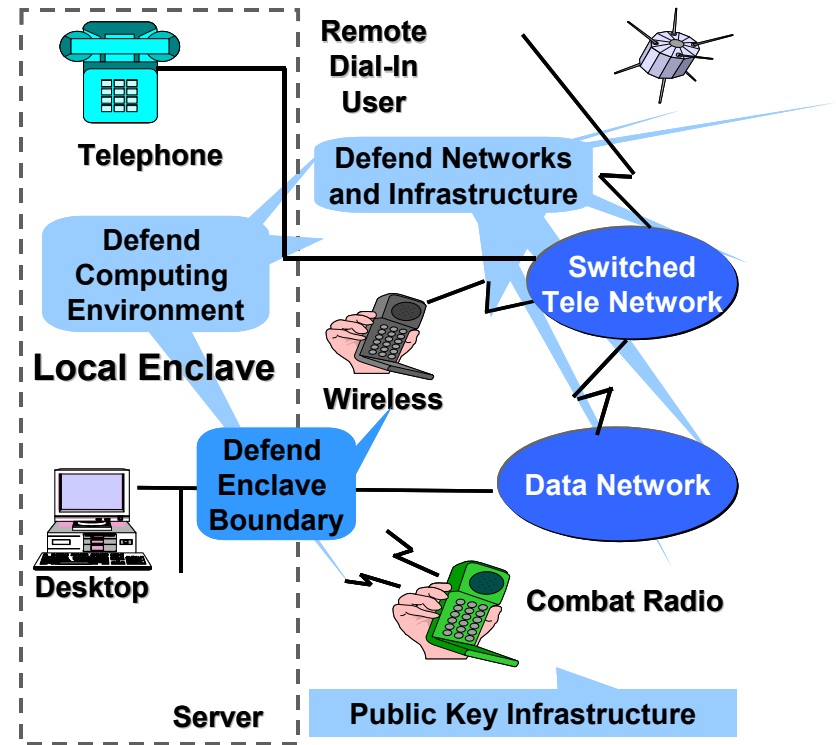
Public Key Infrastructure

The Challenge:
To provide authentication, confidentiality, inter-operability, and access control throughout the enterprise.

Many Players, Many Perspectives

- **Products & Services**
- **Technology**
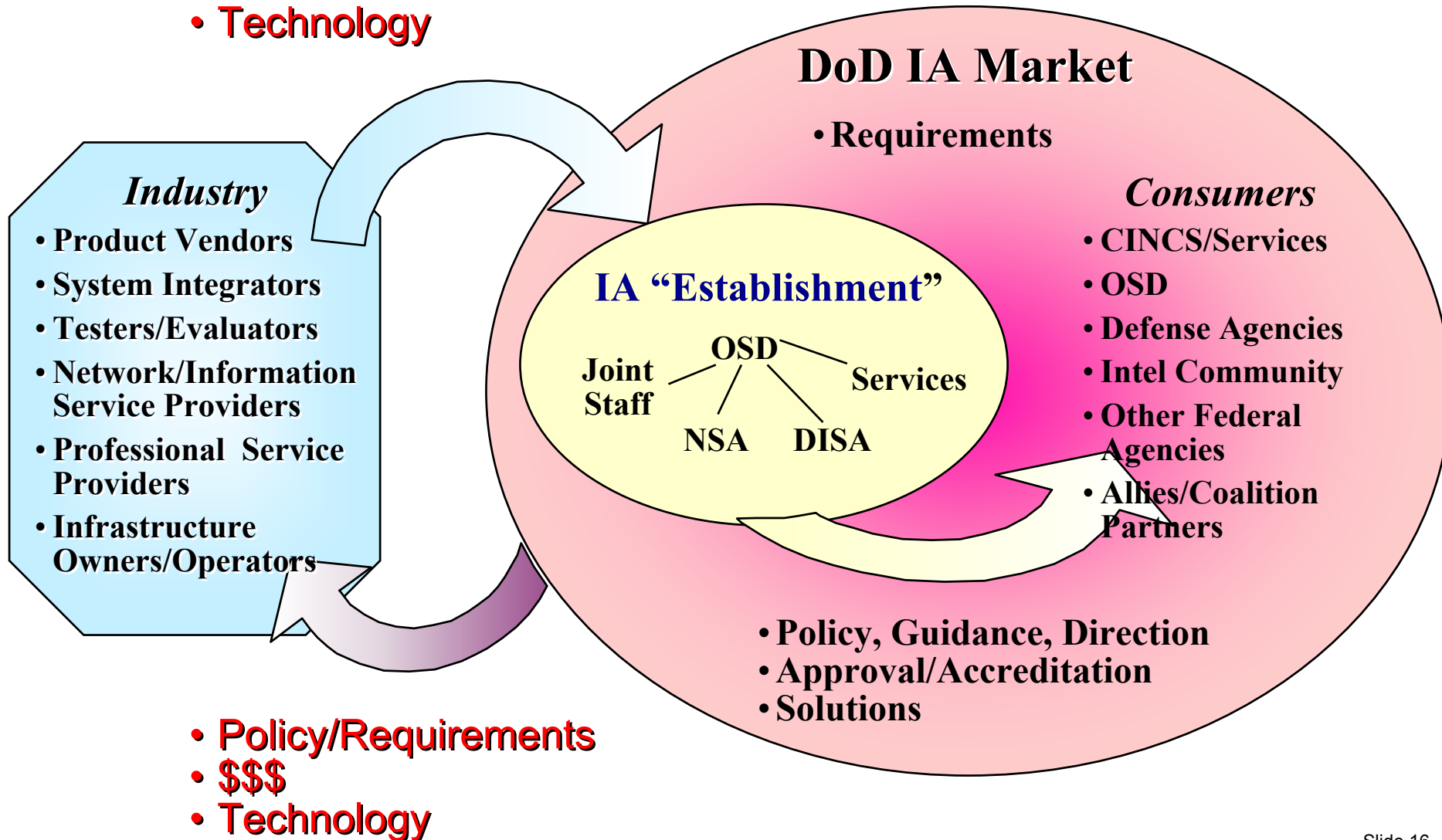
DoD IA Market

- **Requirements**

Industry

- **Product Vendors**
- **System Integrators**
- **Testers/Evaluators**
- **Network/Information Service Providers**
- **Professional Service Providers**
- **Infrastructure Owners/Operators**

IA "Establishment"

OSD
Joint Staff — Services
NSA — DISA

Consumers

- **CINCS/Services**
- **OSD**
- **Defense Agencies**
- **Intel Community**
- **Other Federal Agencies**
- **Allies/Coalition Partners**

- **Policy, Guidance, Direction**
- **Approval/Accreditation**
- **Solutions**

- **Policy/Requirements**
- **$$$**
- **Technology**

DoD's View of Industry

- Commercial users willing to field systems with less than adequate security

- Don't publicize computer security problems

- Most decisions are cost-driven

  - Cost/benefit
  - Insurance
  - Write-off losses
  - Pass loss on to customer

CAVEAT EMPTOR

- Not a lot of leading edge R&D -market focused

- Many vendors lack long-term R&D Vision necessary to solve the hard problems (evolutionary advances - function vice new capabilities)

- Commercial world utilizes high-cost workarounds to implement security solutions

- Virtually all commercial work based on previous DoD research
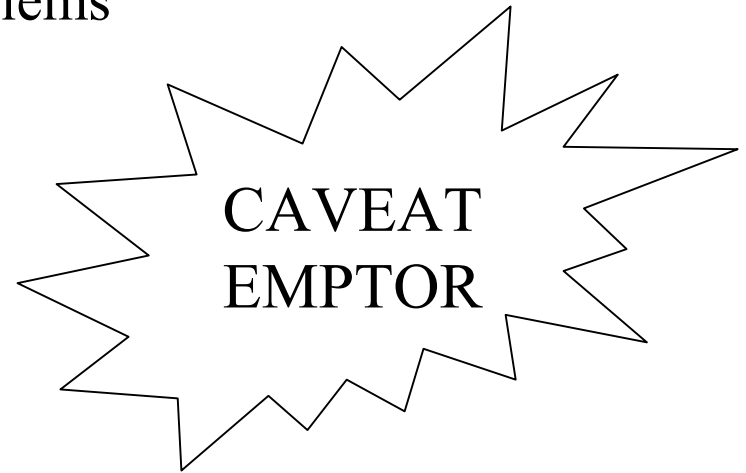
DoD IA Policy

DoDD 8500.aa - Information Assurance (Roles & Responsibilities)

DoDI 8500.bb - IA Implementation

"Managing information assurance as a quality across the IT life cycle - are achieved through core IA initiatives such as the NIAP and the development and use of CCPP and evaluation methods for COTS; through the DITSCAP for all government and contractor information systems connected to the GIG; education, training and awareness for IA and IT professionals and GIG users; the IAVA and other vulnerability management processes; incident response; continuity planning; and consequence management."

•Establishes threshold assurance levels for connection to the GIG

National Information Assurance Partnership
NSTISSIP-11

- Common Criteria (CC) Evolution
- Common Criteria Test Program Commercial Lab Accreditation
- CC Security Target & Protection Profile Generation Support
- Validated Product List Publication
- Test Methods & Tools Development

NIAP
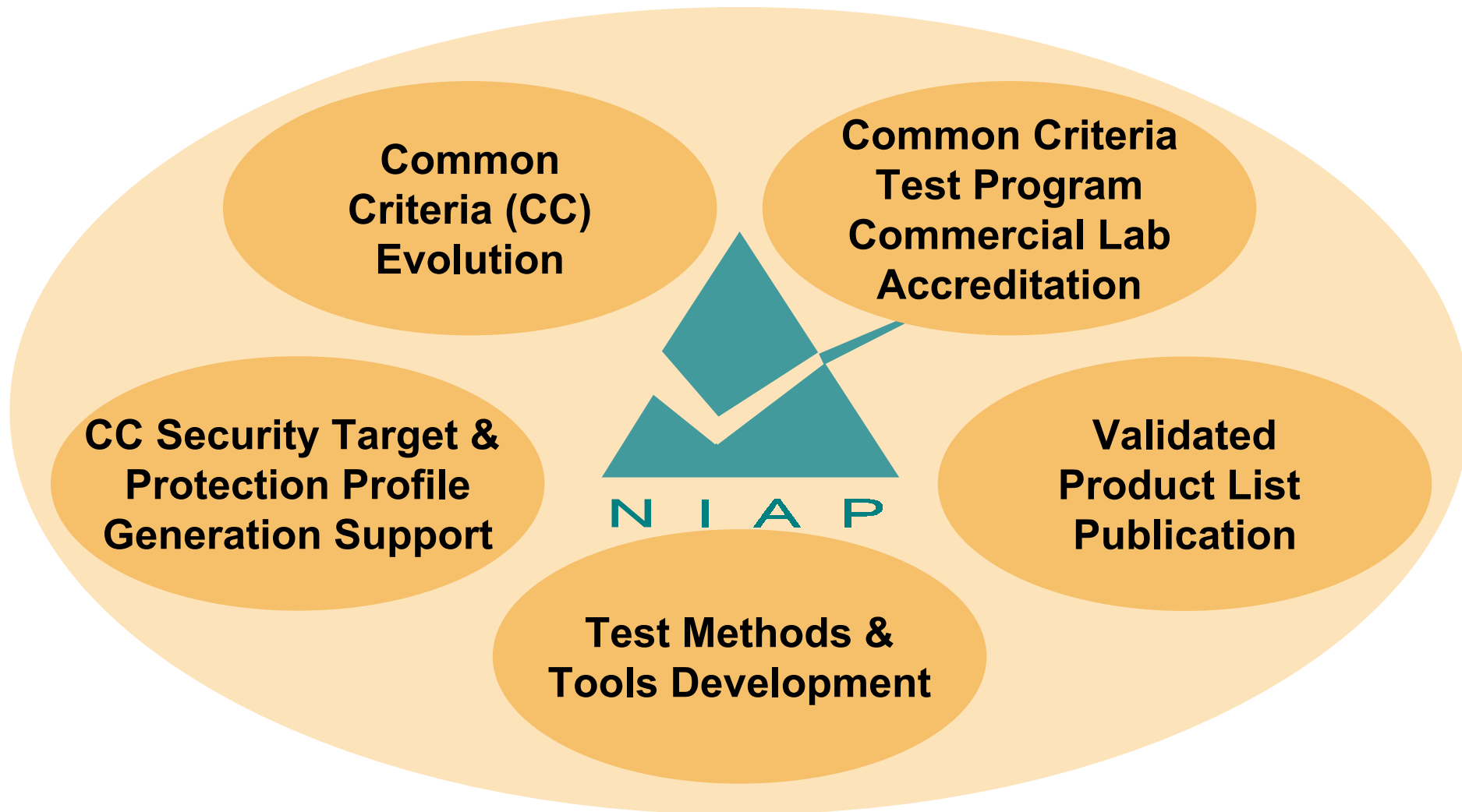
NIST / NSA JOINT INITIATIVE

Slide 19

Strengthening the Links to Enable IA

Four areas where we can help each other...

Create

- Assist in our efforts to innovate (e.g., DARPA, Service Labs)
- Leverage industry's market research w/our resource base
- Help us develop the tools, techniques, procedures for mutual protection

Consolidate

- Assess IA-related efforts in a broader nation-wide context
- Focus on priorities

Commit

- Be part of our solutions
- Find the "common ground" in combating terrorism;

Conduct

- Implement community solutions proven effective for a given environment
- Share best practices and lessons learned

Technology & Solutions

Operations

People

Information Dominance

You are a Critical Piece of the Information Dominance Puzzle

Department of Defense

Business Sector

INFORMATION ASSURANCE

Private Citizens

Government - State, Local, Federal